Nmap Cheat Sheet

Basic Scanning

Command	Description
`nmap <target>`	Scan host (top 1000)
`nmap 192.168.1.0/24`	Scan subnet
`nmap -iL targets.txt`	Scan from file

Host Discovery

Flag	Description
`-sn`	Ping scan only
`-Pn`	Skip discovery
`-PS22,80`	TCP SYN ping
`-PA80`	TCP ACK ping
`-PE`	ICMP echo ping
`-PR`	ARP ping (fastest)

Port Scanning Techniques

Flag	Description
`-sS`	TCP SYN (stealth)
`-sT`	TCP Connect
`-sU`	UDP scan
`-sA`	TCP ACK
`-sN/-sF/-sX`	Null/FIN/Xmas

Port Specification

Flag	Description
`-p 80`	Single port
`-p 80,443`	Multiple ports
`-p 1-1000`	Port range
`-p-`	All 65535 ports
`--top-ports 100`	Top N ports
`-F`	Fast (top 100)

Output Formats

Flag	Description
`-oN file.txt`	Normal output
`-oX file.xml`	XML output
`-oG file.gnmap`	Grepable
`-oA basename`	All formats
`--open`	Only open ports

Service & Version Detection

Flag	Description
`-sV`	Detect versions
`--version-intensity`	0-9 intensity
`-A`	Aggressive scan

OS Detection

Flag	Description
`-O`	Enable OS detection
`--osscan-guess`	Aggressive guess

Timing & Performance

Flag	Description
`-T0`	Paranoid (slow)
`-T1`	Sneaky
`-T2`	Polite
`-T3`	Normal
`-T4`	Aggressive
`-T5`	Insane
`--min-rate 100`	Min pkts/sec

Firewall Evasion

Flag	Description
`-f`	Fragment packets
`--mtu 24`	Custom MTU
`-D RND:5,ME`	Decoys
`-g 53`	Source port
`--spoof-mac 0`	Random MAC

Verbosity

Flag	Description
`-v / -vv`	Verbose
`-d`	Debug
`--reason`	Port reason

Nmap Cheat Sheet

Nmap Scripting Engine (NSE)

Flag	Description
`-sC`	Run default scripts
`--script=<name>`	Run specific script
`--script=<cat>`	Run category
`--script-args`	Pass arguments

NSE Categories

Category	Purpose
`vuln`	Vulnerability detection
`exploit`	Active exploitation
`brute`	Password attacks
`safe`	Non-intrusive
`discovery`	Enumeration

Popular NSE Scripts

Script	Description
`--script vuln`	All vulnerability checks
`--script http-enum`	Web directory enum
`--script smb-vuln*`	SMB vulnerabilities
`--script ssl-enum-ciphers`	SSL/TLS analysis
`--script ftp-anon`	Anonymous FTP check

Common Scan Combinations

Discovery & Enumeration

```
# Network sweep
nmap -sn 192.168.1.0/24
# Service scan
nmap -sV -sC -p- target
# Full CTF scan
nmap -A -T4 -p- target
```

Vulnerability & Stealth

```
# Vuln scan
nmap --script vuln -sV target
# Web enum
nmap --script http-enum -p80 target
# Stealth scan
nmap -sS -T2 -f -D RND:5 target
```

Port States

State	Meaning
`open`	Service accepting connections
`closed`	No service listening
`filtered`	Firewall blocking
`open|filtered`	Cannot determine

Ultimate Full Scan

```
sudo nmap -sS -sU -sV -O -sC -p- -T4 -oA fullscan target
```

Practice These Commands in Real Labs

HackerDNA: 170+ vulnerable machines for hands-on practice
Start free at hackerdna.com/labs